UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/075,016	02/13/2002	Tomoyuki Asano	SONYJP 3.0-239	8582

530 7590 12/06/2005

LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK
600 SOUTH AVENUE WEST
WESTFIELD, NJ 07090

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 12/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/075,016	ASANO, TOMOYUKI	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 October 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 April 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Original application contained claims 1 – 46. Claims 1, 4, 6, 10, 12, 15, 16, 20, 21, 23 – 25, 32, 33, 35, 42 – 44 and 46 have been amended in an amendment filed on 10/11/2005. The amendment filed have been entered and made of record. Presently, pending claims are 1 – 46.

Response to Arguments

2. Applicant's arguments with respect to instant claims have been fully considered but are moot in view of the new ground(s) of rejection necessitated by the amendment of claim limitations.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 2, 12, 13, 21, 23, 25 – 29, 31, 35 – 39, 41, 44 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter (Patent Number: 6253193), in view of Ober (Patent Number: 6307936).

As per claim 1, 12, 21 and 23, Ginter teaches an information playback device for playing back information from a recording medium having encrypted content recorded thereon by a content recording entity, the information playback device comprising:

a cryptosystem unit operable to determine the validity of a public key certificate of the content recording entity, to acquire a public key of the content recording entity from the public key certificate if the public key certificate is valid, and to decrypt the encrypted content if the validity of a digital signature of the content recording entity is verified based on the acquired public key (Ginter: Column 203 Line 58 – 67).

Ginter does not teach whereby the device corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves corresponding to a respective encryption key; and whereby decryption by the device of said decrypted content is selectively inhibited by changing one or more keys corresponding to nodes included in a node path between said leaf corresponding to the device and said root node.

Ober teaches the device corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves corresponding to a respective encryption key (Ober: Column 3 Line 10 – 22, Column 22 Line 25 – 33 and Figure 2 & 4); and

whereby decryption by the device of said decrypted content is selectively inhibited by changing one or more keys corresponding to nodes included in a node path

between said leaf corresponding to the device and said root node (Ober: Column 22 Line 25 – 33: each customer / user key KEK is encrypted by the GKEK (internal protection) as well as LSV (root key of the key-tree) and once a customer key is covered by a GKEK it can not be covered by any other key (Column 22 Line 25 – 33) – i.e. decryption by the device is particularly associated with an unique key in the corresponding path of the key-tree, as taught by Ober, and as such the change of one or more keys in the path – i.e. using different keys other than the pre-determined unique keys would fail to decrypt the content and thereby the decryption by the device of said decrypted content is thus inhibited as to meet the claim language).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ober within the system of Ginter because Ober teaches providing an enhanced key management scheme allowing for efficient access to all keys so that the cryptographic algorithms can run in high speed as well as in a compact form (Ober: Column 1 Line 42 – 45).

As per claim 2 and 13, Ginter as modified teaches the digital signature of the content recording entity is generated by digitally signing the encrypted content, and the cryptosystem unit decrypts the encrypted content if the validity of the generated digital signature is verified (Ginter: Column 247 Line 1 – 5: the PERC (Permission Records) considered as part of the aggregated content portion is encrypted as private header (Ginter: Figure 17) and then digitally signed as a digital signature along with the PERC).

As per claim 25, 35 and 46, Ginter teaches an information playback device for playing back information from a recording medium having encrypted content recorded thereon by a content recording entity, the information playback device comprising: a cryptosystem unit operable to acquire from the recording medium identification data representing the content recording entity, to determine a revocation state of the content recording entity based on the acquired identification data, and to decrypt the encrypted content if the content recording entity has not been revoked (Ginter: Column 203 Line 58 – 67 and Column 204 Line 4 – 26).

Ober teaches the device corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves corresponding to a respective encryption key (Ober: Column 3 Line 10 – 22, Column 22 Line 25 – 33 and Figure 2 & 4); and

whereby decryption by the device of said decrypted content is selectively inhibited by changing one or more keys corresponding to nodes included in a node path between said leaf corresponding to the device and said root node (Ober: Column 22 Line 25 – 33: each customer / user key KEK is encrypted by the GKEK (internal protection) as well as LSV (root key of the key-tree) and once a customer key is covered by a GKEK it can not be covered by any other key (Column 22 Line 25 – 33) – i.e. decryption by the device is particularly associated with an unique key in the corresponding path of the key-tree, as taught by Ober, and as such the change of one or more keys in the path – i.e. using different keys other than the pre-determined unique

keys would fail to decrypt the content and thereby the decryption by the device of said decrypted content is thus inhibited as to meet the claim language).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ober within the system of Ginter because Ober teaches providing an enhanced key management scheme allowing for efficient access to all keys so that the cryptographic algorithms can run in high speed as well as in a compact form (Ober: Column 1 Line 42 – 45).

As per claim 26 and 36, Ginter as modified teaches the cryptosystem unit is operable to determine the validity of a public key certificate of the content recording entity, to acquire data identifying the content recording entity from the public key certificate if the public key certificate is valid, and to determine whether the content recording entity has been revoked based on the identifying data (Ginter: Column 203 Line 58 – 67 and Column 204 Line 4 – 26).

As per claim 27 and 37, Ginter as modified teaches the cryptosystem unit is operable to decrypt the encrypted content if the validity of a digital signature of the content recording entity is verified (Ginter: Column 203 Line 58 – 67).

As per claim 28 and 38, Ginter as modified teaches the cryptosystem unit is operable to determine the validity of a public key certificate of the content recording entity, to acquire a public key of the content recording entity from the public key

certificate if the public key certificate is valid, and to decrypt the encrypted content if the validity of a digital signature of the content recording entity is verified based on the public key (Ginter: Column 203 Line 58 – 67 and Column 204 Line 4 – 26).

As per claim 29 and 39, Ginter as modified teaches the cryptosystem unit is operable to determine the validity of a digital signature of the content recording entity generated by digitally signing the encrypted content, and to decrypt the encrypted content if the digital signature is valid (Ginter: Column 203 Line 58 – 67 and Column 204 Line 4 – 26).

As per claim 31 and 41, Ginter as modified teaches the cryptosystem unit is operable to determine the validity of a public key certificate of the content recording entity, to acquire data identifying the content recording entity from the public key certificate if the public certificate is valid, and to determine whether the content recording entity has been revoked based on a comparison between the identifying data and an identification stored in a revocation list (Ginter: Column 203 Line 58 – 67 and Column 204 Line 4 – 26).

As per claim 44, the claim limitations are met as the same reasons set forth in the paragraph above regarding to claim 1 with the exception of the feature of a revocation list. However, Ginter further teaches a revocation list (Ginter: Column 204 Line 5 – 10).

4. Claims 3, 14, 30 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter (Patent Number: 6253193), in view of Ober (Patent Number: 6307936), and in view of Sprunk (Patent Number: 5754569).

As per claim 3, 14, 30 and 40, Ginter does not teaches the digital signature of the content recording entity is generated by digitally signing a title key which corresponds to the encrypted content, and the cryptosystem unit decrypts the encrypted content if the validity of the generated digital signature is verified.

Sprunk teaches the digital signature of the content recording entity is generated by digitally signing a title key which corresponds to the encrypted content, and the cryptosystem unit decrypts the encrypted content if the validity of the generated digital signature is verified (Sprunk: Column 4 Line 22 – 26).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sprunk within the system of Ginter because Sprunk teaches providing a digital content encryption mechanism by using a more efficient hashing scheme that can minimize the burden of the hashing of the information blocks (Sprunk: Column 4 Line 16 – 20).

5. Claims 4, 5, 15, 32 – 34, 42 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter (Patent Number: 6253193), in view of Ober (Patent Number: 6307936), and in view of Richards (Patent Number: 6069957).

As per claim 4, 15, 32, 33, 42 and 43, Ginter as modified does not disclose expressly the cryptosystem unit is operable to acquire decryption-key-generating data required for decrypting the encrypted content by decrypting, based on the stored keys, an enabling key block composed of data generated by using each key on one node path to encrypt a next adjacent upper key on the one node path.

Richards teaches cryptosystem unit is operable to acquire decryption-key-generating data required for decrypting the encrypted content by decrypting, based on the stored keys, an enabling key block composed of data generated by using each key on one node path to encrypt a next adjacent upper key on the one node path (Richards: Figure 29 and Column 1 Line 25 – 30, Column 17 Line 54 – 60 and Column 18 Line 36 – 40).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Richards within the system of Ginter as modified because Richards teaches providing a more efficient function to structure and distribute the decryption keys to various customers (Richards: Column 4 Line 48 – 51).

As per claim 5 and 34, Ginter as modified teaches the decryption-key-generating data is a master key common to the plurality of different information playback devices or a media key unique to the recording medium (Ober: Column 3 Line 15: LSV (Local Storage Key) used as a root key can be interpreted as the master key to all applications (i.e. leave keys)).

6. Claims 6 – 8, 10, 11, 16 – 18, 20, 22, 24 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter (Patent Number: 6253193), in view of Ober (Patent Number: 6307936), and in view of Ruben (Patent Number: 6138237).

As per claim 6, 16 and 24, Ginter teaches an information recording device for recording information on a recording medium, the information recording device comprising:

a cryptosystem unit operable to encrypt content recorded on the recording medium by a content recording entity, to generate a digital signature of the content recording entity, and to record the encrypted content, the digital signature, and a public key certificate of the content recording entity on the recording medium so as to correspond to one another (Ginter: Column 203 Line 58 – 67).

Ginter does not teach whereby the device corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves corresponding to a respective encryption key; and whereby decryption by the device of said decrypted content is selectively inhibited by changing one or more keys corresponding to nodes included in a node path between said leaf corresponding to the device and said root node.

Ober teaches the device corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves

corresponding to a respective encryption key (Ober: Column 3 Line 10 – 22, Column 22 Line 25 – 33 and Figure 2 & 4); and

whereby decryption by the device of said decrypted content is selectively inhibited by changing one or more keys corresponding to nodes included in a node path between said leaf corresponding to the device and said root node (Ober: Column 22 Line 25 – 33: each customer / user key KEK is encrypted by the GKEK (internal protection) as well as LSV (root key of the key-tree) and once a customer key is covered by a GKEK it can not be covered by any other key (Column 22 Line 25 – 33) – i.e. decryption by the device is particularly associated with an unique key in the corresponding path of the key-tree, as taught by Ober, and as such the change of one or more keys in the path – i.e. using different keys other than the pre-determined unique keys would fail to decrypt the content and thereby the decryption by the device of of said decrypted content is thus inhibited as to meet the claim language).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ober within the system of Ginter because Ober teaches providing an enhanced key management scheme allowing for efficient access to all keys so that the cryptographic algorithms can run in high speed as well as in a compact form (Ober: Column 1 Line 42 – 45).

Besides, Ginter as modified does not disclose expressly to record the encrypted content, the digital signature, and a public key certificate of the content recording entity on the recording medium.

Ruben teaches to record the encrypted content, the digital signature, and a public key certificate of the content recording entity on the recording medium (Ruber: Column 5 Line 45 – 48, Column 19 Line 32 – 35 and Figure 7 & Figure 14).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ruben within the system of Ginter as modified because Ruben teaches an enhanced mechanism for authoring, distributing and using software resources such as digital documents only accessed for authorized purpose (Ruben: Column 1 Line 6 – 13).

As per claim 7, 17 and 22, Ginter as modified teaches a processing unit operable to generate a management table having correspondences among addresses of the encrypted content, the digital signature, and the public key certificate, and to record the management table on the recording medium (Ruben: Column 3 Line 46 – 50 and Figure 14).

As per claim 8 and 18, Ginter as modified teaches the cryptosystem unit is operable to generate the digital signature of the content recording entity by digitally signing the encrypted content, and to record the generated digital signature in association with the encrypted content (Ruben: Column 3 Line 46 – 50 and Figure 14; Ginter: Column 247 Line 1 – 5: the PERC (Permission Records) considered as part of the aggregated content portion is encrypted as private header (Ginter: Figure 17) and then digitally signed as a digital signature along with the PERC).

As per claim 10 and 20, Ginter as modified teaches wherein the cryptosystem unit is operable to acquire encryption-key-generating data required for encrypting the content recorded on the recording medium by decrypting an enabling key block composed of data generated by using each key in the node path to encrypt a next adjacent upper key on the node path (Ober: column 3 Line 1 – 22 and Figure 2 & 4: the leave key must be covered (i.e. encrypted) by the next adjacent upper key (Ober: Column 3 Line 19 – 22 and Column 3 Line 5 – 9).

As per claim 11, Ginter as modified teaches the decryption-key-generating data is a master key common to the plurality of different information playback devices or a media key unique to the recording medium (Ober: Column 3 Line 15: LSV (Local Storage Key) used as a root key can be interpreted as the master key to all applications (i.e. leave keys)).

As per claim 45, Ginter as modified does not disclose expressly a management table having correspondences among addresses of the encrypted content, the digital signature, and the public key certificate.

Ruben teaches a management table having correspondences among addresses of the encrypted content, the digital signature, and the public key certificate (Ruben: Column 3 Line 46 – 50 and Figure 14).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ruben within the system of Ginter

because Ruben teaches an enhanced mechanism for authoring, distributing and using software resources such as digital documents only accessed for authorized purpose (Ruben: Column 1 Line 6 – 13).

7. Claims 9 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter (Patent Number: 6253193), in view of in view of Ruben (Patent Number: 6138237), and in view of Sprunk (Patent Number: 5754569).

As per claim 9 and 19, Ginter as modified does not teach the cryptosystem unit is operable to generate the digital signature of the content recording entity by digitally signing a title key which corresponds to the encrypted content, and to record the generated digital signature in association with the encrypted content.

Sprunk teaches the digital signature of the content recording entity is generated by digitally signing a title key which corresponds to the encrypted content, and the cryptosystem unit decrypts the encrypted content if the validity of the generated digital signature is verified (Sprunk: Column 4 Line 22 – 26).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sprunk within the system of Ginter because Sprunk teaches providing a digital content encryption mechanism by using a more efficient hashing scheme that can minimize the burden of the hashing of the information blocks (Sprunk: Column 4 Line 16 – 20).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LBC

Longbit Chai
Examiner
Art Unit 2131

Primary Examiner
AU 2131
12.1.05